



Qualys Security Conference Mumbai, India

Qualys Container Security

Comprehensive Security for the ever-changing Container Stack

Hari Srinivasan

Director Product Management, Qualys, Inc.



Everybody Loves Containers

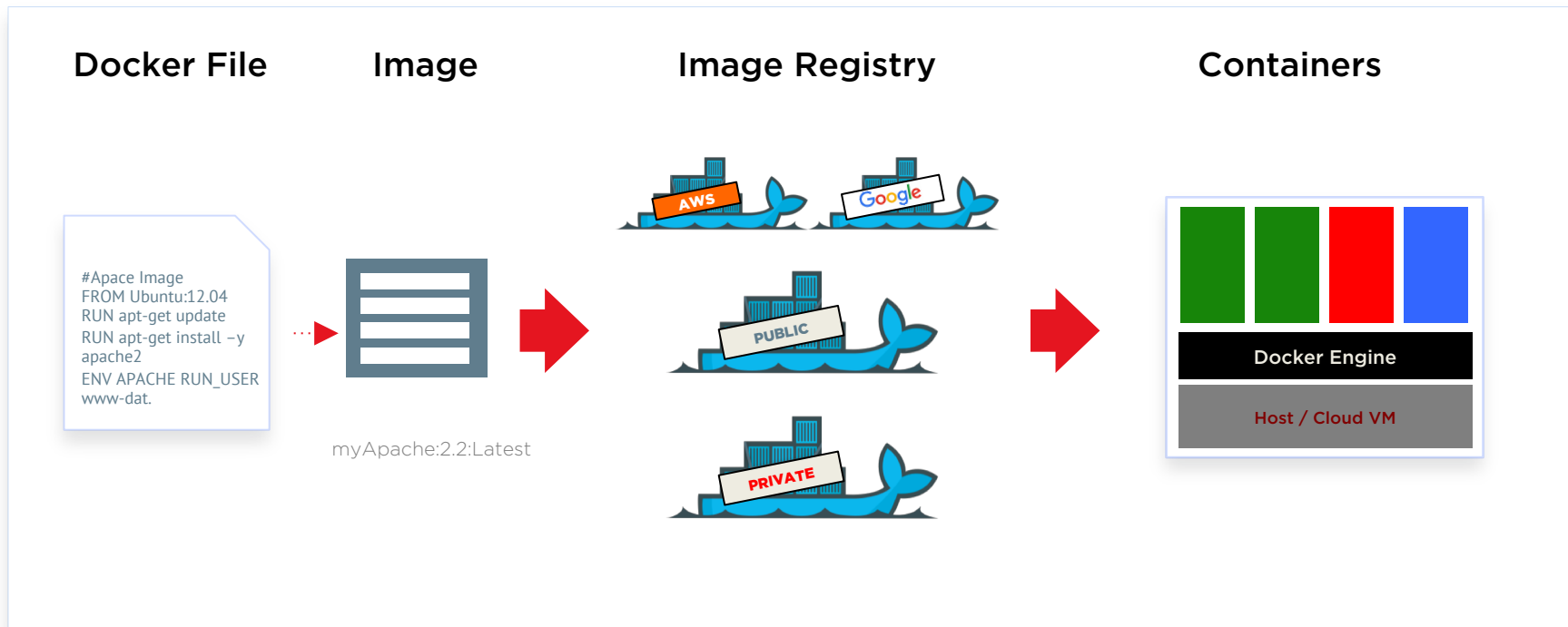


Portability

Agility

Density

Container Components & Lifecycle



Container Platforms

On Premise



Cloud



Azure Container Service



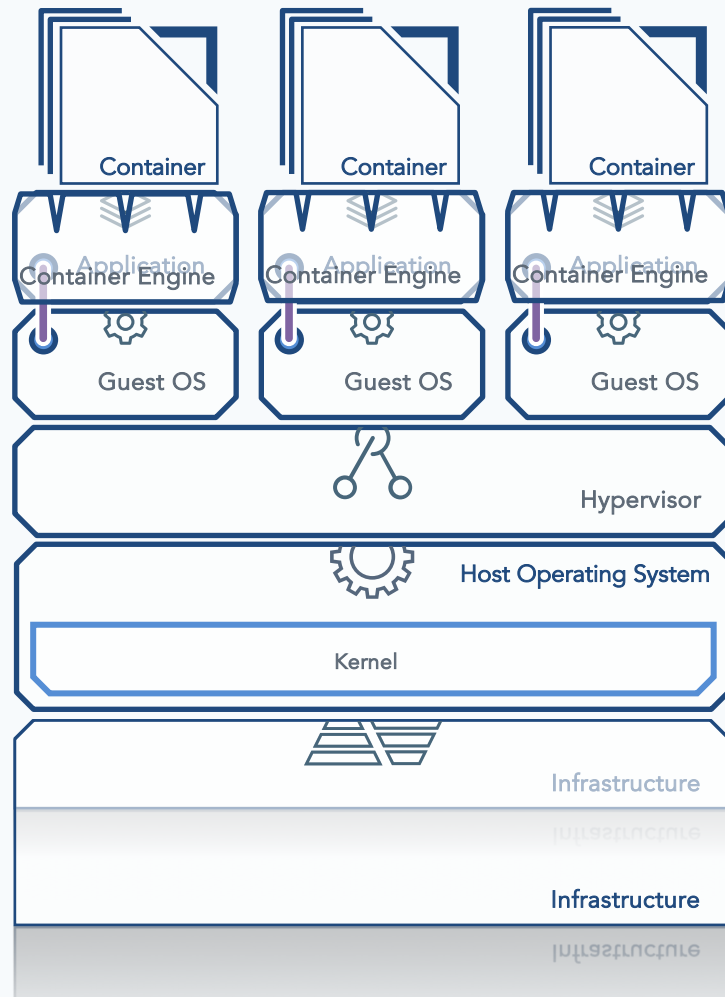
Google Cloud
Container Engine

Container Deployments

Deployment Scenario #1

Use Case

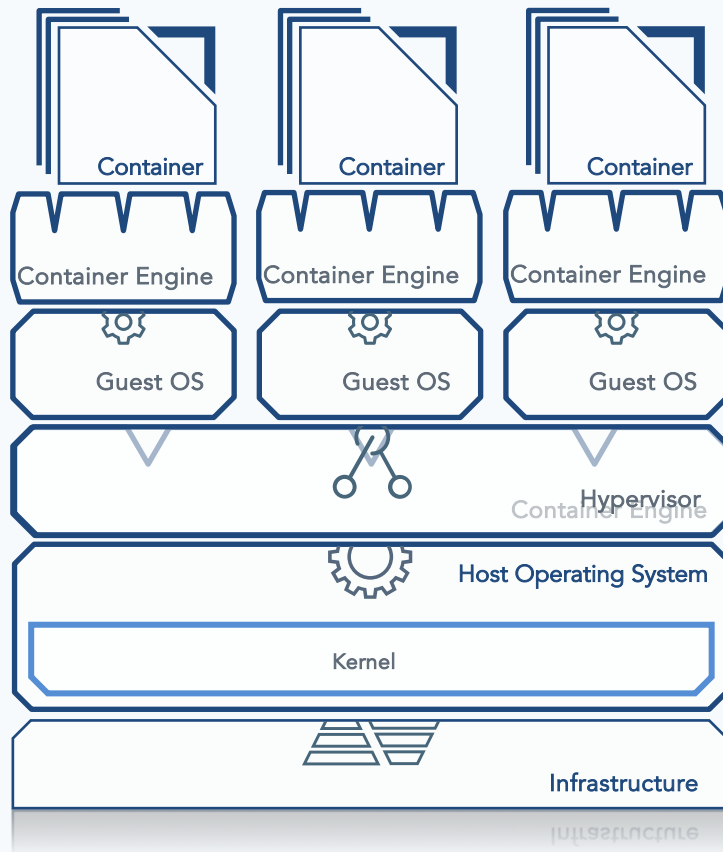
1. Shrinking infrastructure, as organizations continue migration to the cloud
2. Containers deployed within Virtual Machines
3. But organizations still have the overhead and costs of the hypervisor and virtual machines



Deployment Scenario #2

Use Case

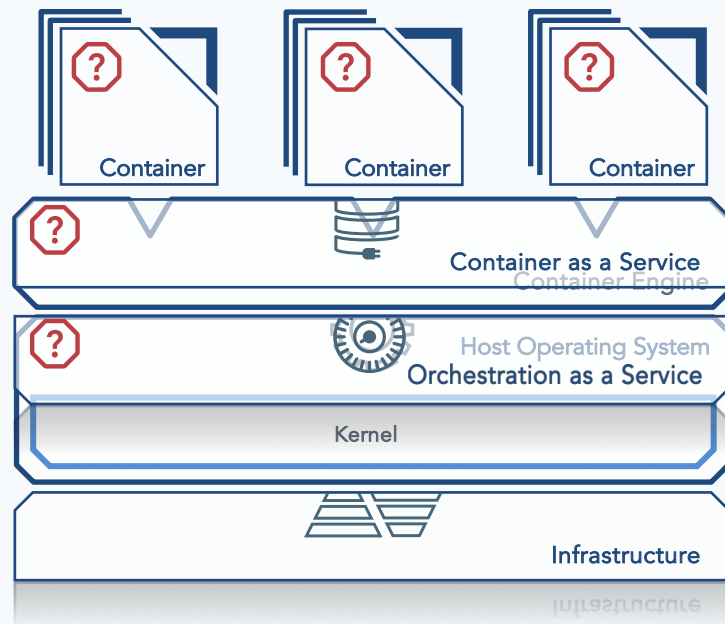
1. The orchestration battle ends with Kubernetes winning 80% of the market
2. But organizations struggle to scale their own Kubernetes clusters



Deployment Scenario #3

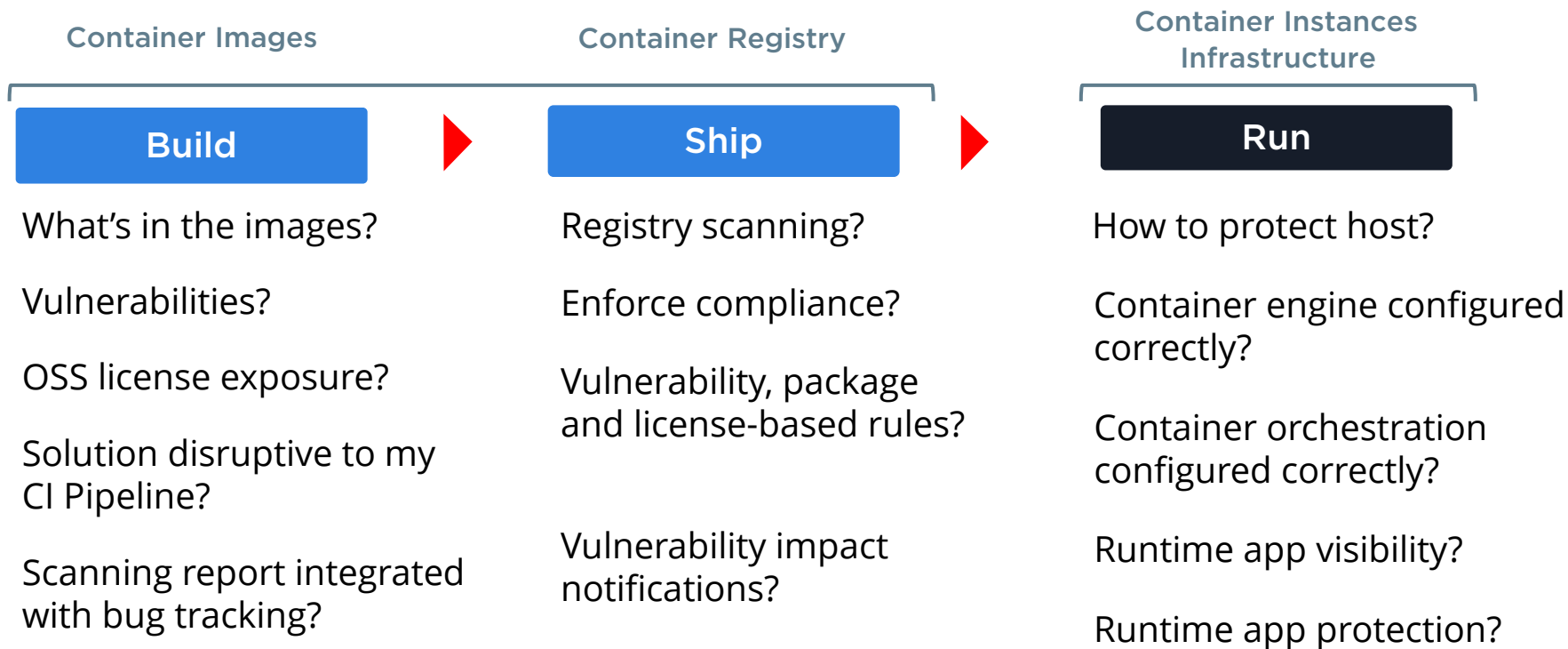
Use Case

1. Container-as-a-Service and Orchestration-as-a-Service adoption accelerate container adoption
2. Now where do you put security?



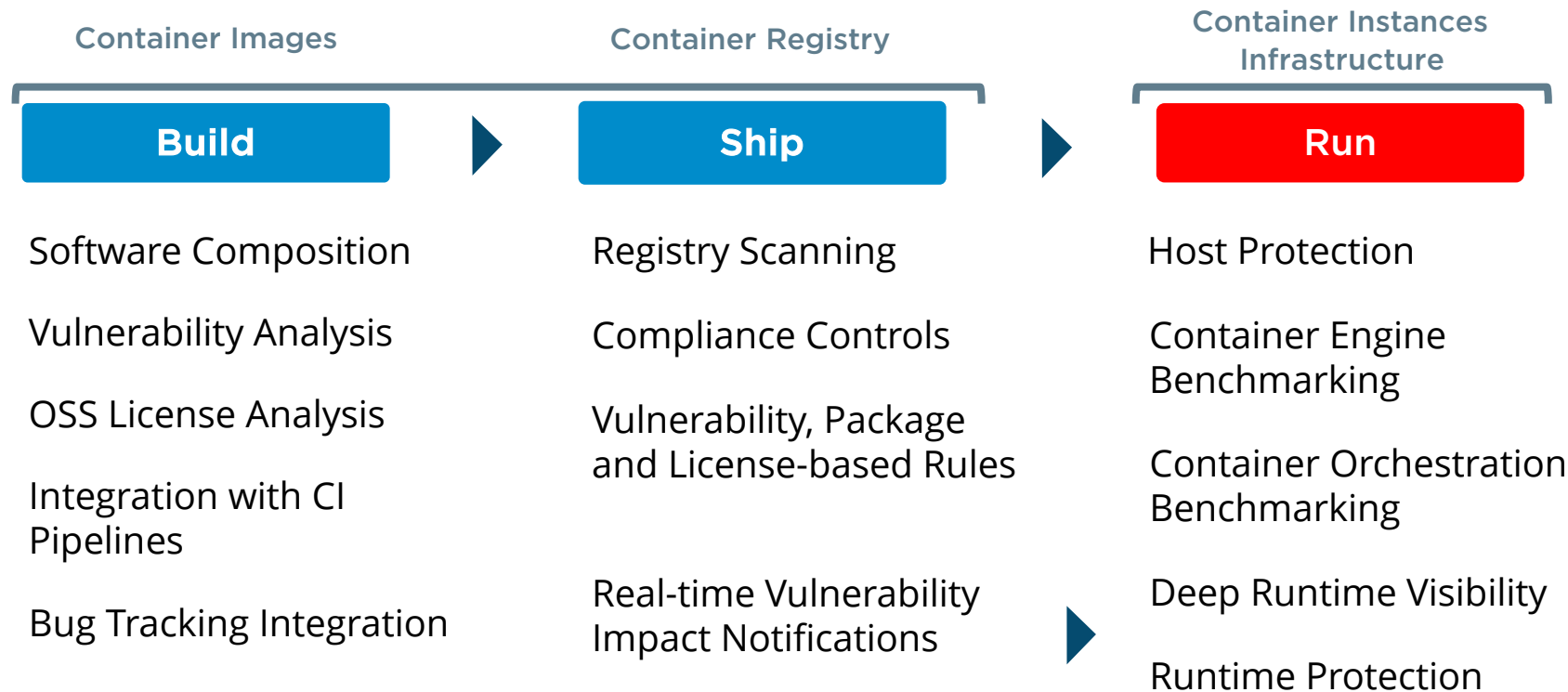
Container Visibility & Security Challenges

Container Lifecycle Challenges



Qualys Container Security

Qualys Container Security



Qualys Container Security

Key Uses



Visibility into your container projects

Identify Hosts with Containers. Inventory of images, containers. Search images with vulnerabilities, labels, tags, packages,.. Build custom widgets.



Secure the CI/CD pipeline

Integrate images, vulnerability scans into the build. FAIL builds, not allowing unsecure images to enter the stream



Scan Registry and block unauthorized images

Inventory and scan as new images are added to the registry. Block unapproved images from being spun up as Containers.



Container Runtime Visibility and Protection

Find what containers are running, know if the runtime got changed from images. Protect from changes or breakouts.

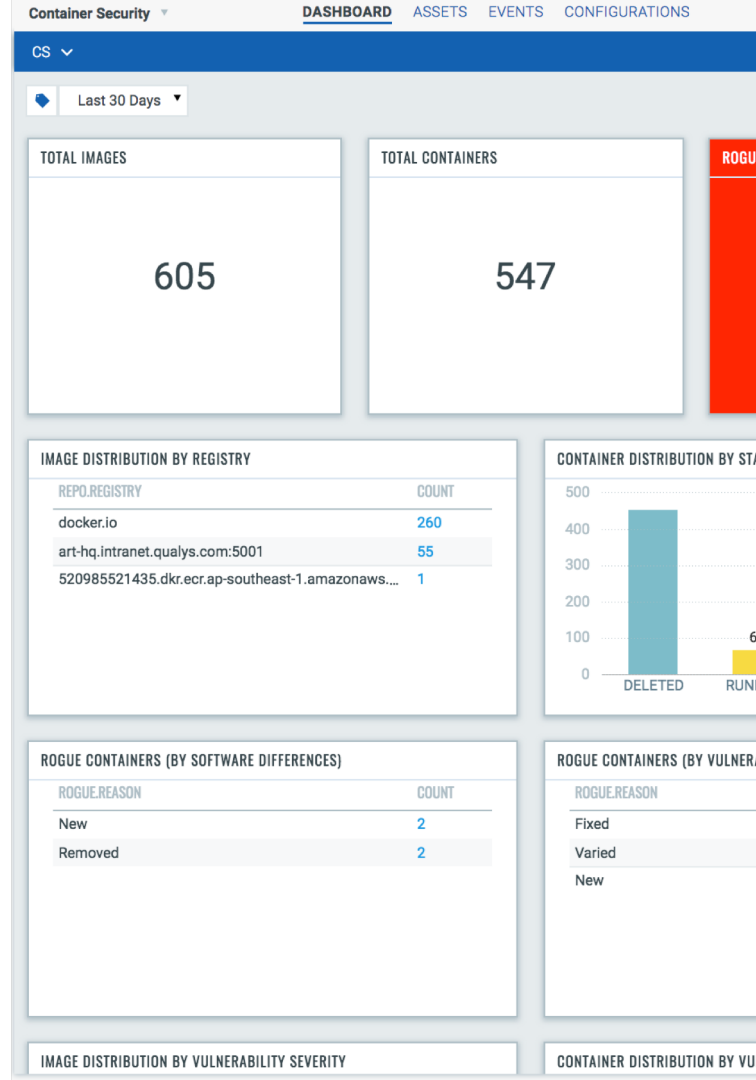
Use Case #1

Visibility into your container projects

Overview Dashboard
Inventory & security posture widgets

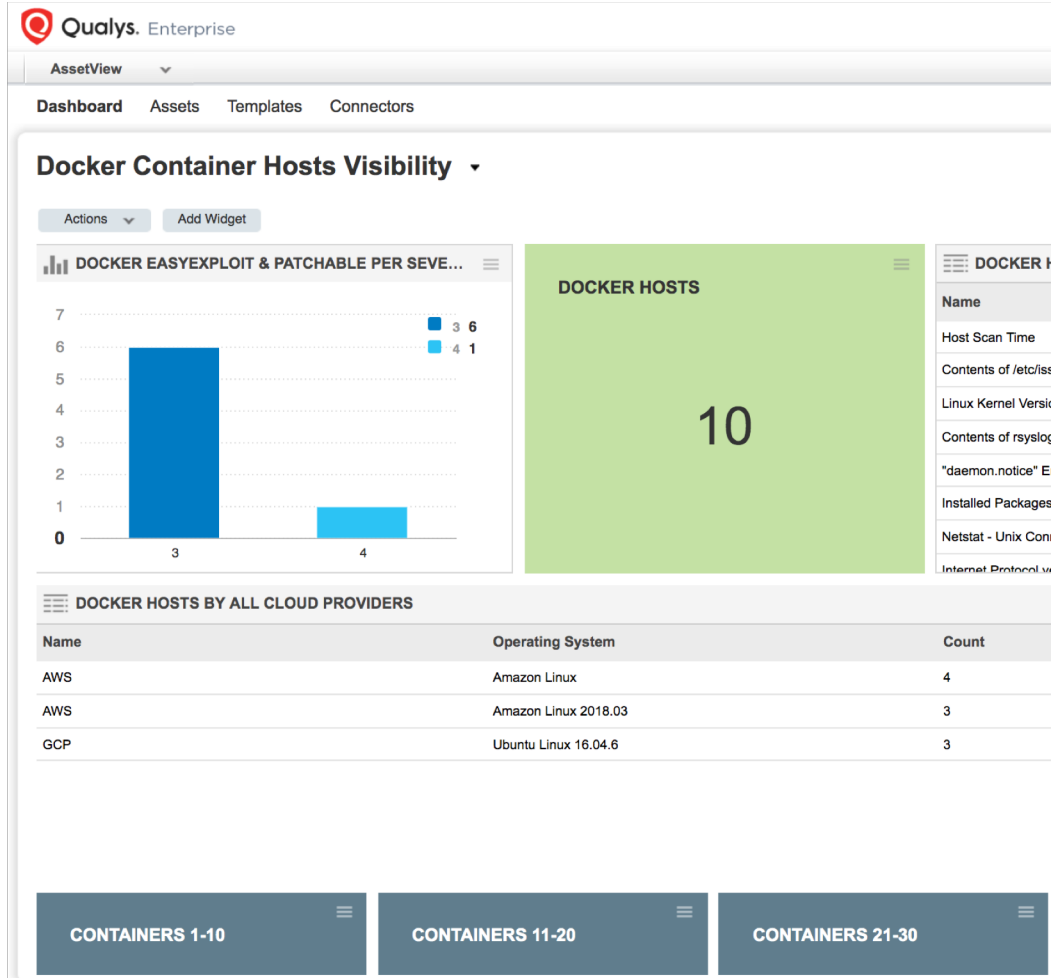
- Container Hosts
- Count of images, containers
- Containers by state
- Vulnerable images

Personalize and add custom widgets



Know where your Containers are?

- Inventory of all Container Hosts across your datacenters, public clouds, laptops,..
- Know how the host vulnerabilities, exploits affect your container environments



Know where your Containers are?

The screenshot shows the AssetView interface with the search bar containing the query `isDockerHost: true`. The results table lists three assets:

Asset Name	OS	Modules	Last Logged-In User	Activity	Sources	Tags
qcs-g-01	Ubuntu Linux 16.04.6	VM PC	amandern	Inventory Scan Complete	Cloud Agent	
qcs-r-1	Ubuntu Linux 16.04.6					
qcs-g2	Ubuntu Linux 16.04.6					

Servers – Datacenter, Clouds, etc..

isDockerHost: "true" and provider: AWS/Azure/GCP

Developer Mac laptops

The screenshot shows the AssetView interface with the search bar containing the query `operatingSystem: mac and software.name: docker`. The results table lists two assets:

Asset Name	OS	Modules	Last Logged-In User	Activity
102354mbp15.local	Mac OS X 10.13.6	VM PC	mquealy	Scan Complete 11 hours ago
101298mbp15.local	Mac OS X 10.13.6	VM	mwalker	Scan Complete 13 hours ago

Image Inventory and Smart Searches

Search based on all attributes

Preset quick search filters - Identify images by application labels

The screenshot shows the 'Assets' page in the Container Security interface. A search bar at the top contains the query: `vulnerabilities.severity:"Severity 5" and repo.registry:"docker.io"`. The left sidebar shows a summary of 68 total images and a list of labels and registries. The main table lists the search results.

REGISTRY	REPOSITORY	CREATED ON	TAGS	CONTAINERS	VULNERABILITIES
docker.io	elasticsearch Image Id: 7b3c18d8f363	Feb 06, 2018	latest	0 On Hosts: 1	2
docker.io	redis Image Id: de560ba5403e	Feb 06, 2018	latest	1 On Hosts: 1	3
docker.io	kibana Image Id: 9ef680b9e227	Feb 06, 2018	latest	0 On Hosts: 1	3
docker.io	node Image Id: a696309517c6	Feb 01, 2018	latest	0 On Hosts: 1	3
docker.io	httpd Image Id: 2e202f453940	Jan 26, 2018	latest	1 On Hosts: 1	3
docker.io	cassandra Image Id: e25e005ebec1	Jan 23, 2018	latest	0 On Hosts: 1	4
docker.io	solr Image Id: 0ee0d104030e	Jan 19, 2018	latest	0 On Hosts: 2	14
docker.io	tomcat Image Id: 66bbcd06c8cd	Jan 18, 2018	latest	0 On Hosts: 1	13
docker.io	kibana Image Id: 6ded4c70c32d	Jan 17, 2018	latest	0 On Hosts: 1	10

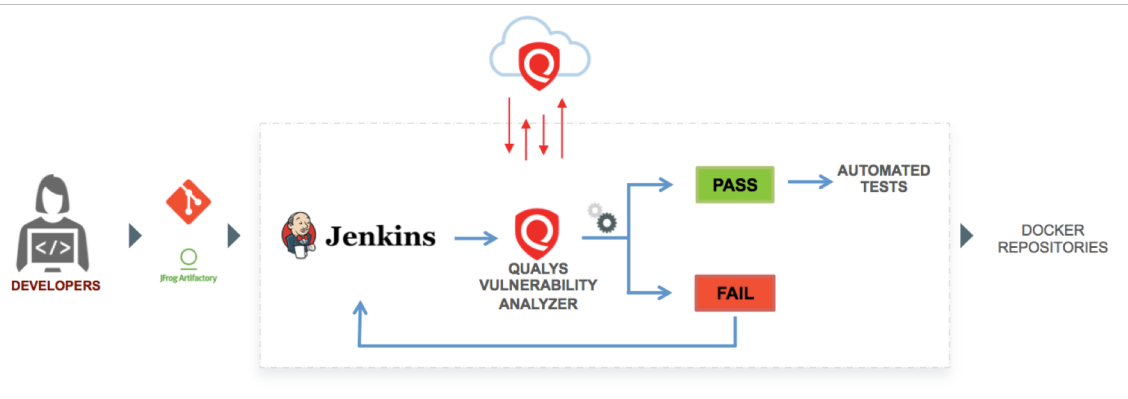
- Image info
- Registry info
- Containers for this image
- Vulnerability posture?
- Easy drill down for complete inventory

Use Case #2



Secure the CI/CD pipeline

Block vulnerable images in the build



Download the **Qualys Vulnerability Analysis plug-in for Jenkins** and install on the Jenkins master

Install the Qualys Container Sensor on the Jenkins worker nodes

Set up policies to Pass/Fail the build. Ex: No Sev.5 vulnerabilities, > CVSS 7, specific QID, vulnerabilities count. Etc.

Plugins:



Jenkins



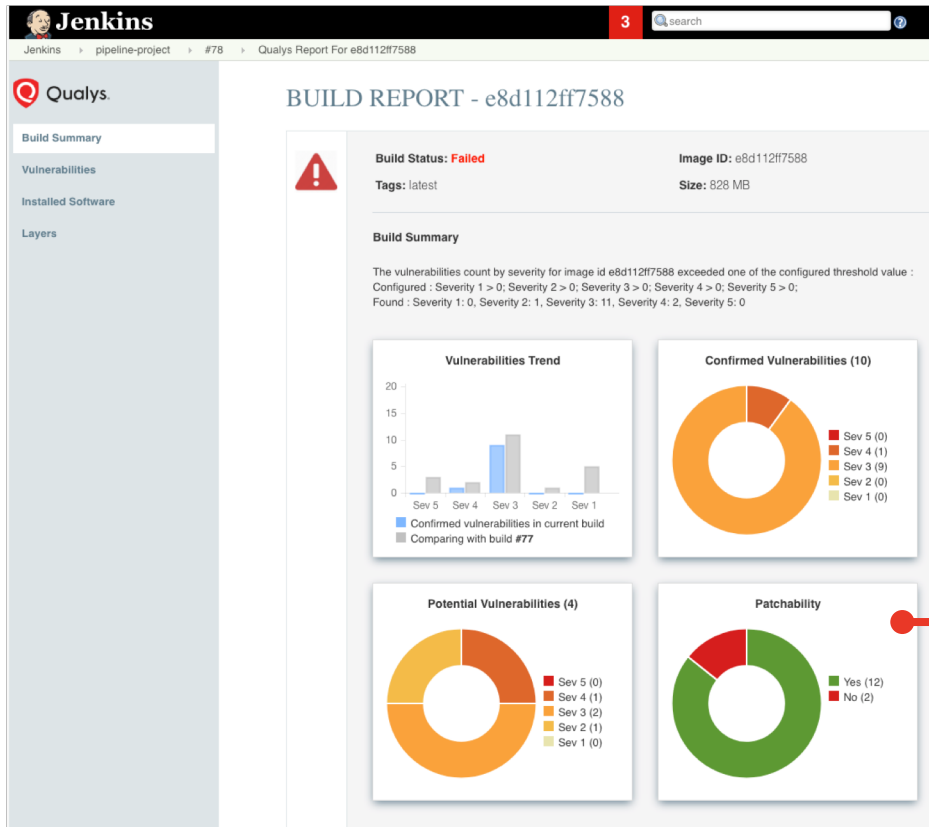
Bamboo



REST APIs for any other integrations.

*,TeamCity, CircleCI - Support coming soon

Actionable Vulnerability Information



Qualys Report For e8d112ff7588

INSTALLED SOFTWARE

Show 10 entries Search: QID=176259

Name	Installed Version	Fixed In Version
libmagickwand-dev	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickwand-6-headers	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickcore-dev	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickcore-6-headers	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
imagemagick-6.q16	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4



Use Case #3

Scan Registry and block unauthorized images

Detect threats from images being shipped

Know your Registries

Vulnerable Images per Registry

REGISTRIES		STATUS	REGISTRY	REPOSITORIES	TOTAL	IMAGES	
						SCANNED	VULNERABLE
Docker.io	100	Running	Docker.io	4	73	35	16
AWS ECR	60	Error	Ubuntu	6	—	—	—
AZURE ECR		Finished	MongoDB	16	154	64	33
GCR		Finished	BusyBot	8	10	5	3
V2							
Artifact							

STATUS	
Completed	3.01K
Running	982
Scheduled	89

Inventory Registry

Qualys. Enterprise
Cloud Security

DASHBOARD ASSETS EVENTS CONFIGURATION g-frame-standard (123)

Configuration Images Containers Registries

160 Sensors

REGISTRIES

- Docker.io 100
- AWS ECR 60
- AZURE ECR
- GCR
- V2
- Artifact

STATUS

- Completed 3.01K
- Running 982
- Scheduled 89

STATUS	REGISTRY	REPOSITORIES	TOTAL	IMAGES SCANNED	VULNERABLE
Running	Docker.io Last scanned on: Apr 21, 2018	4	73	35	16
Error	Ubuntu Last scanned on: Apr 21, 2018	6	—	—	—
Finished	MongoDB Last scanned on: Apr 21, 2018	16	154	64	33
Finished	BusyBot Last scanned on: Apr 21, 2018	8	10	5	3
Running	waf-appliance Last scanned on: Apr 21, 2018	22	22	9	7
Running	oraclelinux Last scanned on: Apr 21, 2018	3	6	6	1

Qualys. Enterprise

← Create New: Registry

STEPS 1/2

- 1 Registry Information
- 2 Scan Settings

Registry Information

Name and select the type for this registry. If Public, add credentials if needed.

REGISTRY TYPE:

Select one...

- AWS ECR
- DockerHub
- Artifactory V2
- Docker Trusted Registry
- Docker V2 Private

PASSWORD:

Cancel Previous Next

* Support coming soon

Setup Scans

Configure scan frequency
for image vulnerability
analysis

Automate scanning of
images every day at a
scheduled time



Qualys. Enterprise

← Create New: Registry

STEPS 1 / 2

- 1 Basic Information
- 2 Scan Settings

Scan Settings

Choose scan type to set scan setting parameters.

PULL SCHEDULE:

On Demand ▼

On Demand

Automatic

On Demand: The sensor will do a one-time pull and scan of repositories/images from the registry.

REPOSITORY:

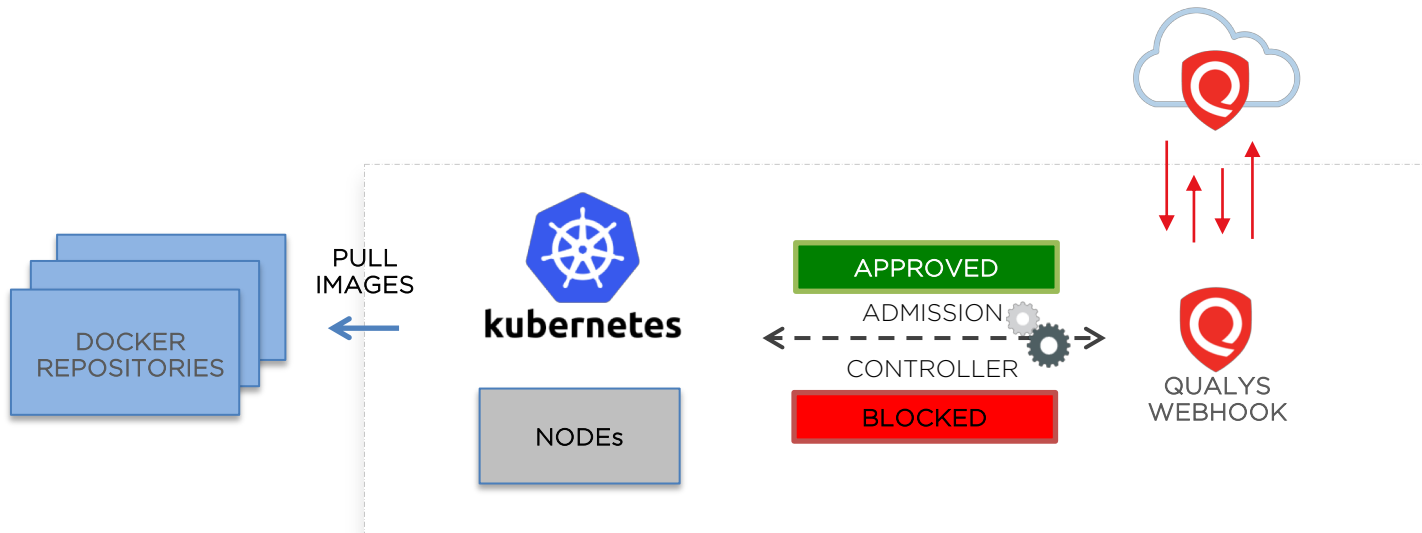
Repository name

Cancel Launch

* Support coming soon

Policy based Orchestration

Blocking unapproved images spun up as containers

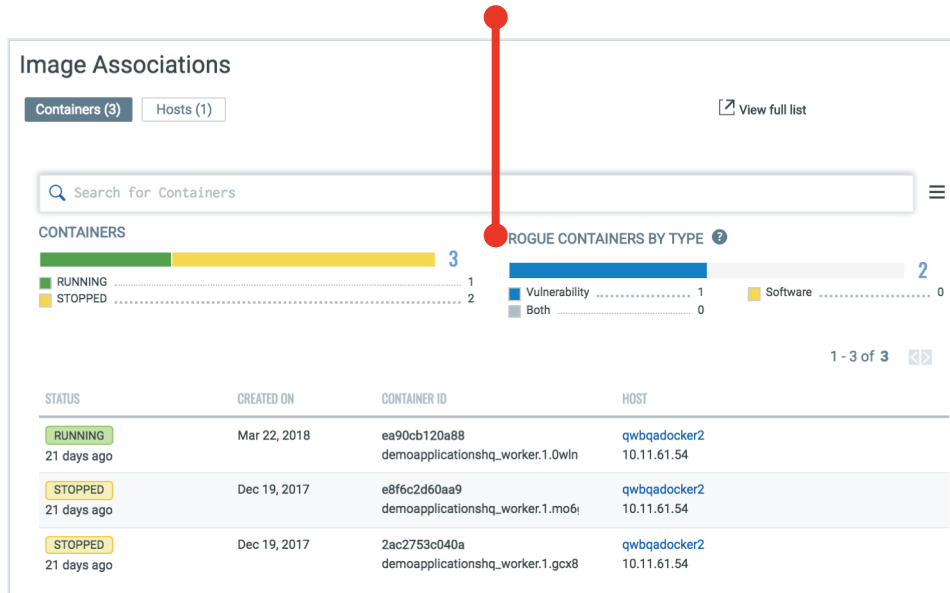


Runtimes Drifts & Protection

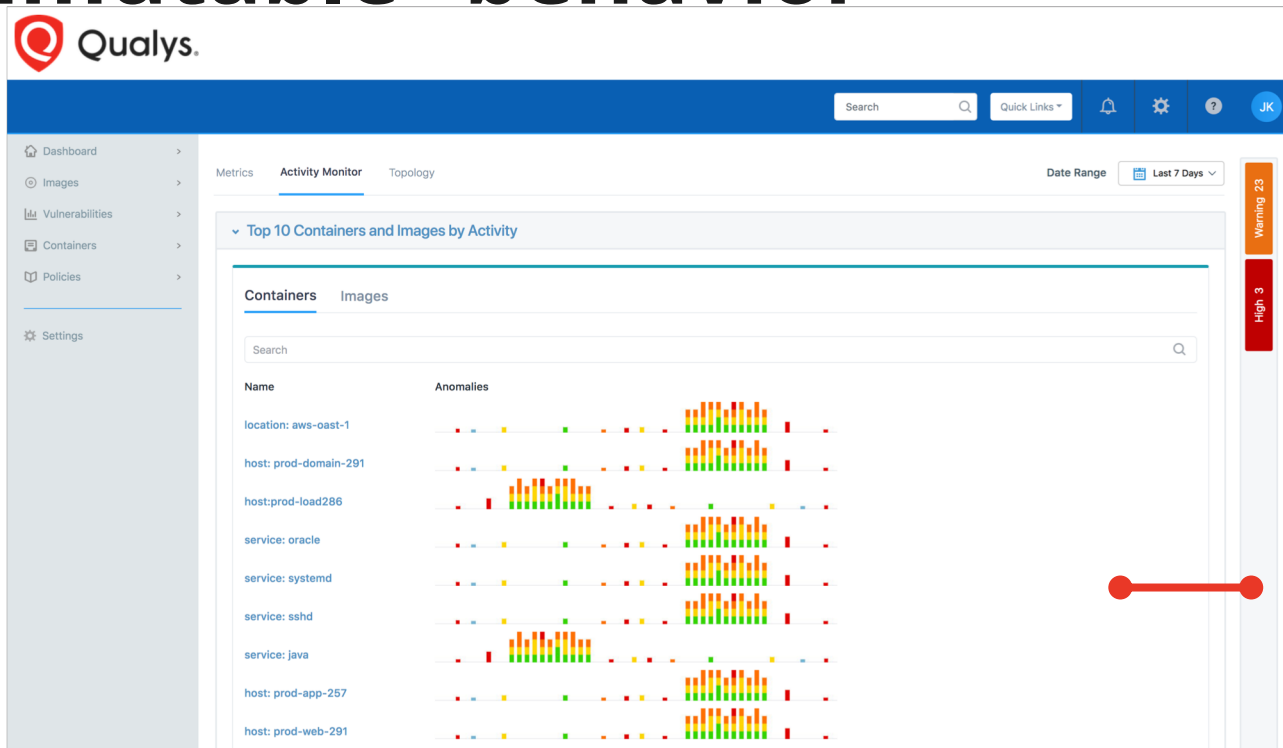
Detect Containers breaking off from “immutable” behavior and Block/Kill/Quarantine them.

Identify potential breaches in containers

“Rogue” Containers, differ from their parent Images by vulnerability, software package composition, behavior, etc



Containers breaking off from the “immutable” behavior



Drill down to the details,
Identify activity in
the containers

Search



Quick Links ▾



JK

Dashboard >

Images >

Vulnerabilities >

Containers >

Policies >

Settings

Metrics

Activity Monitor

Topology

Date Range

Last 7 Days ▾

Container Details



Just now

sys_read



sys_write



sys_open



sys_close



sys_stat



sys_fstat



sys_lstat



sys_writev



sys_pipe



Warning 23

High 3

Event Details ?



Process /usr/sbin/httpd was blocked from executing /bin/sh. Severity: High

Raw log:

Process	Process ID	Call	Arguments	Action	Time
/usr/sbin/httpd	31	sys_execve	/bin/sh	Deny	11/13/2018, 12:48:23AM

Processes executing /usr/sbin/httpd:

- /usr/sbin/httpd

Processes accessing /usr/sbin/httpd:

- /usr/sbin/httpd

Qualys Container Security

Host Protection

CIS Benchmarks

Protection for container
infrastructure stack

Scanning & Compliance

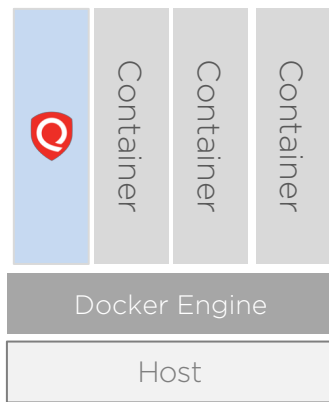
Accurate insight and control
of container images

Visibility & Protection

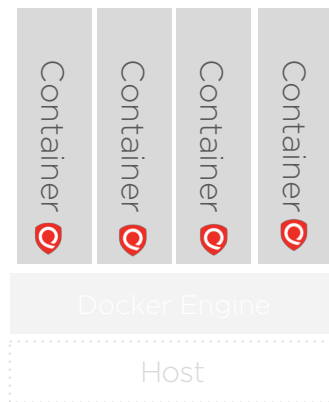
Automated analysis and
enforcement of container behavior

Qualys 'Container Security' Sensor Options

Qualys Container Sensor
Side-car*



Qualys-Layered Insight
Embedded option



* Qualys side-car to 'all' containers on the node. Runs today as non-privileged. As features of compliance and enforcements are added the mode will change to Privileged, with option to revert to non-privileged

Sensors for every use case

PRE-DEPLOYMENT PHASE

POST-DEPLOYMENT PHASE



* Layered In option for runtime protection

** Prevention from starting off malicious containers



Qualys Security Conference Mumbai, India

Thank You

Hari Srinivasan
hsrinivasan@qualys.com